Atty. Dkt. No. 051373-0118 (24)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | |
|---|---|
| Appellants: Tang et al. | **CERTIFICATE OF FACSIMILE TRANSMISSION**<br>I hereby certify that this paper is being facsimile transmitted to the United States Patent and Trademark Office, Alexandria, Virginia on the date below |
| Title: SYSTEM FOR AND METHOD OF PROTECTING A USERNAME DURING AUTHENTICATION OVER A NON-ENCRYPTED CHANNEL | *Todd A. Rathe*<br>(Printed Name) |
| Appl. No.: 10/074,625 | (Signature) |
| Filing Date: 02/13/2002 | (Date of Deposit) |
| Examiner: Patel, Chirag R. | |
| Art Unit: 2141 | |

**BRIEF ON APPEAL**

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

**1. Real Party in Interest**

The real party in interest is Infowave Software, Inc., a British Colombia company corporation having a principal place of business at 4664 Lougheed hwy, Suite 200, Burnaby, BC.

**2. Related Appeals and Interferences**

There are no related appeals or interferences that will directly affect, be directly affected by, or have a bearing on the present appeal, that are known to Appellants or Appellants' patent representative.

**3. Status of Claims**

Claims 1-20 were originally pending in the application. In response to a Final Office Action mailed on June 14, 2006, Appellants filed a request for continuing examination (RCE) on August 15, 2006 requesting amendments to claims 1, 10 and 14. This is an appeal from the non-final Office Action mailed on October 25, 2006 rejecting claims 1-20. The present appeal is directed to Claims 1-20, i.e., all of the presently pending claims that stand rejected in this application.

**4. Status of Amendments**

Since this Appeal follows a first Office Action following the filing of a request for continuing examination (RCE) and an accompanying response to an earlier Final Office Action, all previously requested amendments after Final have been entered.

**5. Summary of Claimed Subject Matter**

Claims 1, 10 and 14 are directed to a method, process and system, respectively, wherein a client or user communicates authentication information including plain text unencrypted information AND an obscured username over a nonsecure or plain text communication channel.

Claim 1 recites a method of protecting a username. The method includes (1) obtaining a plain text username over a secure communication channel (Figure 2, step 210; page 6, lines 17 -20); (2) obtaining a server identifier for a server (Figure 2, step 210; page 6, line 16-20); (3) obscuring the plaintext username using the server identifier (Figure 2, step 230; page 6, lines 21-22); (4) providing the security username and the plaintext username to the server (Figure 2, step 240 semi: page 7, lines 4-6); and (4) communicating authentication information including plain text unencrypted information and the obscured username over a non-secure communication channel from a client (page 6, lines 11-15; Page 8, lines 28-30; page 9, lines 22-27).

Claim 10 recites a username protection process which includes (1) registering a user with a selected server by requesting and receiving a plaintext user identifier

(Figure 3, step 310; page 7, lines 12-16), creating an obscure version of the plaintext user identifier, and storing a plaintext user identifier and the obscure version of the plaintext user identifier on the selected server (Figure 3, step 320; page 7, line 17-18); and (2) initiating a communication session between a user and a selected server by the communication of the obscure version of a plain text user identifier and plain text unencrypted information over a plain text communication channel (page 6, lines 11-15; Page 8, lines 28-30; page 9, lines 22-27).

Claim 14, recites a system for protecting username during authentication over a non-encrypted channel. The system includes a client device (Figure 4, 410) configured to communicate plain text unencrypted information over unsecure communication channels with an obscured user identifier (page 6, lines 11-15; Page 8, lines 28-30; page 9, lines 22-27). The system further recites a server (Figure 4, 450) having stored therein a plain text user identifier communicated by the client device over a secure communication channel and the obscured user identifier corresponding to the plaintext user identifier (page 7, lines 4-6).

## 6. Grounds of Rejection to be Reviewed on Appeal

The issues on appeal are whether the Examiner erred in rejecting Claims number 1-20 under 35 U.S.C. § 102(e) as being as being anticipated by U.S. Patent Publication No. 2002/0157019 (Kadyk et al.).

## 7. Argument

### I. Legal Standards- Law of Anticipation

Claims 1-20 have been rejected under 35 U.S.C. § 102(b), which states:

> A person shall be entitled to a patent unless –
>
> ...
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or

> on sale in this country, more than one year prior to the date of the application for patent in the United States,
>
> ....

Under Section 102, a claim is anticipated, i.e., rendered not novel, when a prior art reference discloses every limitation of the claim. In re Schreiber, 128 F.3rd 1473, 1477 (Fed. Cir.1997). Although a prior art device "may be capable of being modified to run the way the apparatus is claimed, there must be a suggestion or motivation in the reference to do so." In re Mills, 916 F.2d 680, 682 (Fed. Cir. 1990). "Rejections under 35 U.S.C. § 102(a) are proper only when the claimed subject matter is identically disclosed or described in the prior art." In re Arklely, Eardley, and Long, 172 U.S.P.Q. 524, 526 (CCPA 1972).

Claim terms will be given their ordinary and accustomed meaning, unless there is "an express intent to impart a novel meaning to [the] claim [term]" by the patentee. York Prods., Inc. v. Cent. Tractor Farm & Family Ctr., 99 F.3d 1568, 1572 (Fed. Cir. 1996); Sage Prods. v. Devon Indus., Inc., 126 F.3d 1420, 1423 (Fed. Cir. 1997). The ordinary and accustomed meaning of a claim term is determined by reference to dictionaries, encyclopedias, and treatises available at the time of the patent. See Texas Digital Systems, Inc., 308 F.3d at 1203. Such references are always available for claim construction purposes and are neither extrinsic nor intrinsic evidence. See Texas Digital Systems, Inc. v. Telegenix, Inc., 308 F.3d 1193, 1202-03 (Fed. Cir. 2002).

In order to impart a specific meaning to a claim term, i.e., for the inventor to be her own lexicographer, such lexicography must appear "with reasonable clarity, deliberateness, and precision." In re Paulsen, 30 F.3d 1475, 1480 (Fed. Cir. 1994). However, intrinsic evidence may be consulted to determine the definite meaning of a claim term that is unclear. CCS Fitness, Inc. v. Brunswick Corp., 288 F.3d 1359, 1367 (Fed. Cir. 2002). A claim term may be redefined without any express statement of redefinition in the specification. Bell Atl. Network Servs., Inc. v. Covad Communications Group, Inc., 262 F.3d 1258, 1268 (Fed. Cir. 2001). "[A] claim term will not carry its ordinary meaning if the intrinsic evidence shows that the patentee distinguished that term from prior art on the basis of a particular embodiment" or

"described a particular embodiment as important to the invention."

**II. The Examiner's Rejection of Claims 1-20 under 35 U.S.C. § 102(e) as being as being anticipated by U.S. Patent Publication No. 2002/0157019 (Kadyk et al.) Should Be Reversed Because Kadyk et al. Does Not Disclose Every Limitation of Each of the Claims.**

The claimed invention is not anticipated under § 102 unless each and every element of the claimed invention is found in the prior art. (Hydratech, Inc. v. Monochronal Antibodies, Inc., Fed. Cir. 1986). Accordingly, the rejection of these claims under 35 U.S.C. § 102(b) is improper and should be reversed.

Claim 1 recites a method of protecting a username. The method includes a step of communicating authentication information including plain text unencrypted information and an obscured username over a nonsecure communication channel from a client.

Claim 10 recites a username protection process which includes initiating a communication session between a user and a selected server by the communication of the obscure version of a plain text user identifier and plain text unencrypted information over a plain text communication channel.

Claim 14, as amended, recite a system for protecting username. The system includes a client device configured to communicate plain text unencrypted information over unsecure mutation channels with an obscured user identifier. Thus, each of Claims 1, 10 and 14 recite a method, process or system wherein an obscured user identifier or username along with plain text unencrypted information is communicated over an unsecure communication channel.

Kadyk fails to disclose or suggest a method, process or system wherein an obscured user identifier or username is communicated with plain text unencrypted information over an unsecure channel. In contrast, the system disclosed by Kadyk always communicates the username or user identifier over a secure or encrypted channel such that none of the information communicated with the username or user identifier is plain text. In attempting to reject Claims 1 and 10, the Examiner asserts that Kadyk discloses the communication of an obscured username or user identifier

over a non-secure communication channel or plain text communication channel by referring to Paragraphs 12, 13 and 60 and 61 of Kadyk et al..

However, Paragraphs 12, 13 and 60-62 of Kadyk et al. do not disclose the communication of an obscured or encrypted username or user identifier over a nonsecure or plain text channel. Paragraphs 12 and 13 merely disclose, in the background section of Kadyk et al., the known method of tunneling. As described by Kadyk et al. and as known to those of ordinary skill in the art, the process of tunneling does not involve communicating an obscured or encrypted username or user identifier over an unsecure or plain text communication channel. As clearly set forth in Paragraph 12, "in tunneling, the proxy receives an encrypted message from the client that is addressed to a server.... Operating on behalf of the client, the proxy forwards the encrypted message to the server." (Emphasis added). Thus, the entire message is encrypted. Nowhere do Paragraphs 12 and 13 disclose that an obscured username is communicated along with plain text information over an insecure unencrypted channel.

Paragraphs 60 and 61 also fail to disclose the communication of an obscured username or user identifier over an insecure communication channel. Paragraph 1661 merely disclose a step for authenticating a user at client 5022 proxy 504. Although paragraphs 60 and 61 recites an insecure client-proxy connection, this insecure client-proxy connection is only established after authentication between the client and the proxy has been completed over a secure communication channel. A complete reading of Kadyk et al. in context reveals that what Kadyk et al. discloses, at most, is a process including the steps of (1) establishing a secure connection between a client and a proxy for the exchange of authentication data (i.e. a user identifier), (2) the proxy negotiating a secure end-to-end communtication between the client and a server, (3) downgrading the client-proxy channel from a secure channel to an unsecure channel once the secure end-to-end channel has been negotiated with the server. (See paragraphs 61-63 of Kadyk et al.). In other words, the user identifier or username is always communicated over a secure channel.

Paragraph 62 of Kadyk et al. also fail to disclose the communication of an obscured username or user identifier over an insecure communication channel. In contrast, all information communicated from the client is encrypted to some degree. Although information communicated between the client and the proxy server is over an "insecure client-proxy connection," this insecure client-proxy connection encapsulates a secure end-to-end client/server connection. As a result, all information transmitted across the insecure client-proxy connection is already encrypted. As noted in Paragraph [0018] of Kadyk et al.:

> The additional layer of protection provided by the secure client-proxy connection is now redundant and the proxy downgrades the connection so that it is no longer encrypted. The client and server encrypt all data they exchanged through the tunnel, and one level of encryption is sufficient.

In response to such previous points, the Examiner once again attempt to rely upon Kadyk et al. by arguing that:

> Kadyk et al. discloses per [0060], "The step for authenticating a user may include HTTP basic authentication, HTTP digest authentication, or some other type of authentication, such as authentication based on a client certificate that is exchanged at a time the secure client-proxy connection is established." Digest reads on claim limitations "obscured username".

(Office Action dated October 25, 2006; pg. 2).

However, the same paragraph [0060] cited by the Examiner also subsequently states:

> Once the client is authenticated, the client and proxy performs the step of altering the secure client-proxy connection to be insecure, as shown at reference 540. For example, the client-proxy connection can be made insecure by performing the act of setting the encryption used by the connection to a no cipher.

(Kadyk et al., Paragraph [0060]) (Emphasis added). Thus, Paragraph [060] is crystal clear that during such authentication, when the client 502 is authenticated to the

proxy 504, the client proxy connection is secure, i.e. encrypted. Thus, an obscured username is not communicated along with plain text unencrypted information over an insecure channel. Accordingly, the rejection of claims 1, 10 and 14 based upon Kadyk et al. should be reversed. The rejection of claims 2-9, 11-13 and 15-20, which depend from Claims 1, 10 and 14, respectively, should be reversed for the same reasons.

## Conclusion

In view of the foregoing, the Appellants submit that Claims number 1-20 are not properly rejected under 35 U.S.C. § 102(e) as being as being anticipated U.S. Patent Publication No. 2002/0157019 (Kadyk et al.) and are therefore patentable. Accordingly, Appellants respectfully request that the Board reverse all claim rejections and indicate that a Notice of Allowance respecting all pending claims should be issued.

**Summary**

For the foregoing, it is submitted that the Examiner's rejections are erroneous, and reversal of the rejections is respectfully requested.

Dated this 26th day of March, 2007.

Respectfully submitted,

P.O. Address:
RATHE PATENT & IP LAW
10611 W. Hawthorne Farms Lane
Mequon, WI 53097
Telephone: (262) 478-9353

By Todd A. Rathe

Todd A. Rathe
Registration No. 38,276

## CLAIMS APPENDIX

1. (Previously Presented) A method of protecting a username during authentication, the method comprising:

obtaining a plain text username over a secure communication channel;

obtaining a server identifier for a server;

obscuring the plain text username using the server identifier;

providing the obscured username and the plain text username to the server; and

communicating authentication information including plain text unencrypted information and the obscured username over a non-secure communication channel from a client.

2. (Original) The method of claim 1, wherein the server identifier is a uniform resource locator (URL) corresponding to the server.

3. (Original) The method of claim 1, wherein the server identifier is an authentication domain corresponding to the server.

4. (Original) The method of claim 1, wherein obscuring the plain text username using the server identifier comprises encrypting the plain text username using an encryption method.

5. (Original) The method of claim 1, wherein the encryption method is advanced encryption standard (AES).

6. (Original) The method of claim 1, wherein the client is a wireless device.

7. (Original) The method of claim 1, wherein obtaining a plain text username over a secure communication channel comprises establishing an encrypted communication session between the user and the server and communicating a plain text username from the user to the server.

8. (Original) The method of claim 1, wherein the authentication information satisfies a plain text, unencrypted authentication scheme.

9. (Original) The method of claim 1, wherein the server identifier is a combination of an authentication domain and a uniform resource locator (URL) of the server.

10. (Previously Presented) A username protection process comprising:

registering a user with a selected server by requesting and receiving a plain text user identifier, creating an obscure version of the plain text user identifier, and storing the plain text user identifier and the obscure version of the plain text user identifier on the selected server; and

initiating a communication session between the user and the selected server by the communication of the obscure version of the plain text user identifier and plain text unencrypted information over a plain text communication channel.

11. (Original) The process of claim 10, wherein the user is a wireless client device communicating over a non-encrypted channel.

12. (Original) The process of claim 10, wherein communication over a plain text channel involves the obscure version of the plain text user identifier and communication over a secure channel can use the plain text user identifier.

13. (Original) The process of claim 10, wherein the obscure version of the plain text user identifier is stored on the user device.

14. (Previously Presented) A system for protecting a username during authentication over a non-encrypted channel, system comprising:

a client device being configured to communicate plain text unencrypted information over unsecure communication channels using an obscured user identifier; and

a server having stored therein a plain text user identifier communicated by the client device over a secure communication channel and the obscured user identifier corresponding to the plain text user identifier.

15. (Original) The system of claim 14, further comprising a registration device being configured to communicate information over secure communication channels.

16. (Original) The system of claim 15, wherein the client device and registration device are the same device.

17. (Original) The system of claim 14, wherein the client device does not encrypt communication when communicating with the obscured user identifier created from the plain text user identifier.

18. (Original) The system of claim 14, wherein the client device has stored therein the plain text user identifier and the obscured user identifier.

19. (Original) The system of claim 14, wherein the obscured user identifier corresponding to the plain text user identifier is created by encrypting the plain text user identifier with a key.

20. (Original) The system of claim 19, wherein the key is based on the uniform resource locator (URL) of the server or an authentication domain of the server.

## EVIDENCE APPENDIX

There is no evidence previously submitted under 37 C.F.R. §§ 1.130, 1.131 or 1.132 or other evidence entered by the Examiner and relied upon by Appellant in this appeal. Accordingly, the requirements of 37 C.F.R. §§ 41.37(c)(1)(ix) are satisfied.

## RELATED PROCEEDINGS APPENDIX

There are no decisions rendered by a Court of the Board in a proceeding identified in the Related Appeals and Interferences section. Accordingly, the requirements of 37 C.F.R. §§ 41.37(c)(1)(x) are satisfied.